RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

IT BACKUP

FUNDAMENTALS

ANSSI-BP-100-EN
27/11/2025

TARGETED AUDIENCE:

Developers **Administrators** **IT security managers** **IT managers** Users

Information

Warning

This document, written by ANSSI, the French National Cybersecurity Agency, is titled **"IT Backup"**. It is freely available at `cyber.gouv.fr/en`.
It is an original creation from ANSSI and it is placed under the "Open Licence v2.0" published by the Etalab mission.
According to the Open Licence v2.0, this document can be freely reused, subject to mentionning its paternity (source and date of last update). Reuse means the right to communicate, distribute, redistribute, publish, transmit, reproduce, copy, adapt, modify, extract, transform and use, including for commercial purposes
The recommendations are provided as is and are related to threats known at the publication time. Considering the information systems diversity, ANSSI cannot guarantee direct application of these recommendations on targeted information systems. Applying the following recommendations shall be, at first, validated by IT administrators and/or IT security managers.
This document is a courtesy translation of the initial French document **"Titre non défini"**, available at `cyber.gouv.fr`. In case of conflicts between these two documents, the latter is considered as the only reference.

Document changelog:

VERSION	DATE	CHANGELOG
1.0	18/10/2023	Initiale version
1.1	27/11/2025	Minor revision

Contents

1
Context

At the time of publication, ransomware remains a significant cyber threat [1]. All entities are at risk of suffering opportunistic or targeted attacks from a cybercriminal group. The backup of information systems, initially useful in the event of operational incidents (e.g: hardware breakdown), is now essential to ensure efficient responses to security incidents.

Attackers frequently attempt to encrypt, erase, or render unavailable the backup infrastructure, seeking to slow down the restoration of the affected information system and, therefore, to increase their chance of getting the ransom.

The recommendations provided in this document are aimed at securing the backup infrastructure put in place. They must be considered on a case-by-case basis, depending on the context, size, and criticality of the information system to be protected. Recommendations **in bold** are considered to be the most critical and of the highest priority.

1. *2024 Cyber Threat Overview* available on https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-003/.

2
Reminders

- Backup strategies must notably consider the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) defined for all of the business values of the entity's information system (data application)[2].
- Some use cases are not covered by backup, for example:
  - the need for RPO within 24 hours: in this case, other solutions, such as replication (synchronous or asynchronous), must be favoured;
  - the need for legal archiving, which can sometimes imply a need for data authenticity (which is not necessarily covered by backup solutions).
- The essential components of a backup infrastructure are:
  - backup catalogue/index which lets you know what is being backed up;
  - backup software agent installed on the servers being backed up;
  - backup server which processes the backup data stream before sending it to a storage medium;
  - backup storage media: disks, magnetic tapes, USB external disk, etc.
- Backup strategies must define the retention times for backups. This strategy specifies the long-term retention periods - for example, 15 days for daily backups, 1 year for monthly backups, 5 years for annual backups.
- A so-called 'offline' backup is a backup made on a medium which is disconnected from any information system. Magnetic tape is still the most effective medium for this purpose.
- The backup operator must be considered as an administrator with high privileges on the information system. It is therefore important to be vigilant when it comes to determining the level of trust granted to these operators, and to include specific security clauses in the event of subcontracting.

2. See also the ISO/IEC 27031:2011 standard: 'Guidelines for the preparation of communication and information technologies for business continuity' (in French '*Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité*').

3
Recommendations

3.1 IT architecture

R1 **Backup servers need to be segmented and located within the administration information system, or at least in a network zone kept separate from the production environment hosting the backup servers.**

R2 **Backup traffic must transit through the administration network.**

R3 **Backup traffic must transit through a dedicated logical subnet (VLAN).**

R4 **A backup server instance and a data shop should be dedicated to each level of data and/or application sensitivity.** For example, the following elements must have a dedicated backup instance:

- the administration information system;
- systems storing secrets (e.g. directory, key management infrastructure, secure secret vault);
- workstations, if these need to be backed up.

R5 **Servers which host the backup infrastructure cannot be part of a production Windows domain (Active Directory). They must have an independent authentication system (local accounts, directory dedicated to administration).**

R6 **Backup traffic must be strictly filtered by means of an internal firewall.**

R7 In particular, datamart [3] must only be accessible from backup servers.

R8 Backup traffic must be initiated by the server to the clients being backed up.

R9 If backup infrastructure is obsolete but must nevertheless be retained, it should be kept offline in a secure condition. Whenever its reconnection is required, it must be done from a network that is logically disconnected or partitioned from the rest of the information system.

R10 Actions carried out on backup infrastructure must be logged and centralised on an event log collector.

3. A datamart is a set of organised and consolidated data designed to meet a business need; it is a subset of a data warehouse.

3.2 Operations

R11 The "3 – 2 – 1" rule should be applied: 3 copies of the backup - i.e., the one in production and 2 backups stored on distinct media -, among which one is offline.

R12 **It is essential to set up an offline backup (or at least an off-site online backup under certain conditions), even if it is performed less frequently than regular online local backups (see table 2 in section 3.5).**

R13 Backup operations are administrative tasks and must therefore follow the best practices outlined in ANSSI's secure administration guide.

R14 **Each backup instance must have dedicated administrator accounts.**

R15 **Administrator accounts for backup must be named and dedicated.**

R16 Depending on the capabilities of the software, the roles of backup operators (RBAC [4]) should be segmented by defining at least an operational role (daily tasks) and an advanced administration role (strategy and configuration).

R17 Technical backup accounts (used, for example, to run software agents) must be secured: system privileges should be limited to the bare minimum, and credentials must be regularly and preferably automatically renewed.

R18 Users should not be allowed to directly perform backups or restorations on the information system (a feature which is sometimes offered by certain software providers). This presents a risk of unauthorised data access and privilege escalation within the information system [5]. § If such a need exists, usage should be strictly controlled (by limiting authorised users), and all actions should be logged.

R19 The "cross-restore" feature should be disabled [6] by default on the backup software.

R20 **Every component of the backup infrastructure must be proactively updated (including backup software, firmware, etc.). It is advisable to monitor CVEs and the security advisories issued by the software vendor**.

R21 Backups must always be subject to verification by backup operators. This check should include a checklist to detect unusual behaviour: inconsistent data or file volumes, network slowdowns, changes to backup policy configurations, etc.

R22 Backups should be tested regularly. A system restoration procedure must be drawn up and regularly implemented.

R23 An appropriate restoration strategy and order must be defined, paying particular attention to the following criteria: the information system's dependency on infrastructure services (DNS, NTP, directory services, etc.), the criticality of business applications, the duration of restoration and data resynchronisation, and the restoration method (virtual machines, Bare Metal Recovery (BMR [7], etc.).

4. *Role based access control*.
5. For example, a malicious user might restore a known /etc/shadow file onto a targeted server.
6. A backup server instance must not be able to restore from a data store or media referenced by another instance.
7. *Bare Metal Restore*, a full restoration of a physical server.

R24 **In the event of a security incident, the primary response must be to isolate the backup infrastructure from the rest of the information system. This requires an "emergency containment" mechanism (e.g., an automated script or physical disconnection *via* a switch).**

R25 **It is important to back up installation media and the configurations of business applications.**

R26 The backup of the backup infrastructure must be considered. It should include, as a minimum: binaries to deploy minimal infrastructure (operating systems, software, and relevant patches), procedures to import backups, the backup catalogue, a hardware inventory for deployment at a disaster recovery site, and—if the data is encrypted by the backup software—the procedures for importing the encryption keys.

R27 Following a security incident, backups may contain attacker implants (e.g., malicious code, backdoors). This risk must be considered when rebuilding the information system. To minimise impact, restored elements should be verified and, wherever possible, handled in a granular manner:

- reinstalling business applications using vendor-signed binaries;
- carrying out configuration compliance checks before restarting applications;
- scanning business data for malware prior to importing it into production;
- maintaining a consistent backup history aligned with business requirements.

3.3 Data protection

R28 Backup data transfers must be secured using encryption and mutual authentication between client and server, based on industry best practice (e.g., TLS).

R29 **The level of protection for backup data (e.g., encryption strength) must be aligned with the level of protection applied to the same data in the production environment.**

R30 If backups are encrypted, encryption key management must be addressed: who holds the keys, how they are stored (e.g., in a secure vault), and how they are themselves backed up (ideally offline).

R31 **If the physical security of a backup site is deemed insufficient, backups must be encrypted by default (including hard drives, magnetic tapes, etc.).**

R32 Before decommissioning or disposing of backup media, secure erasure must be performed (e.g., deletion of encryption keys, data zeroisation [8]), or the media must be physically destroyed (e.g., shredded or incinerated).

8. Sequencing of multiple random data write operations to the storage medium

3.4 Virtualisation

In the context of virtualisation, it should be assessed whether it is more appropriate to backup the virtual machine's disk image directly or to install the backup agent within the virtual machine. This assessment should take into account the following criteria:

- the volume of data modified on the virtual machine during each backup;
- the required level of granularity in the restoration process;
- whether or not the virtual machine is encrypted (depending on the tools used, this may require decryption and re-encryption, thereby exposing data in plaintext);
- the ability to rebuild the virtual machine from scratch (e.g., via automation).

Table 1 lists the advantages and disadvantages of each option. A hybrid approach is also possible: performing full virtual machine backups at a lower frequency, and more frequent backups of data within the virtual machine.

	Virtual machine disk file backup	Installation of the agent within the virtual machine
Advantages	■ The backup operator does not have access to the contents of the virtual machine, if encrypted. ■ Backup volume can potentially be optimised if virtual machine deployment is automated, with a clear distinction between "live" (data, logs) and "static" disks (operating systems, applications).	■ Possible granularity for file backup and restoration. ■ Consistency of operations when backing up physical servers as well.
Disadvantages	■ Restoration may present difficulties when restarting certain applications (such as databases or Active Directory) or may be unsuitable for specific restoration requests (for example, file servers). ■ Performance issues can occur with block-level deduplication backups if the virtual machine is encrypted.	■ Increased attack surface on backed up servers (local agent with elevated privileges). ■ The backup operator may have access to unencrypted data on the backed up servers.

Table 1 – Advantages and disadvantages by virtual machine backup method

If backup servers are virtualised, they must be co-hosted exclusively with servers of a sensitivity level equivalent to that of the administrative information system.

3.5 Outsourcing

Table 2 outlines the key risks and potential solutions for backups in environments not controlled by the organisation (e.g., public cloud hosting, subcontracting):

	Off-site (online)	Off-site (offline)
Risks	Vigilance regarding the sensitivity of backed up data: ■ Location of backups within the European Union (pay attention to the internal replication of the hosting provider in the case of "online" backups); ■ Encryption of backups using entity-specific methods before sending them to the host or service provider. Vigilance regarding restoration time in line with the RTO requirements: ■ Time to availability of the backup in both cases: > contractual priority in the case of "online" (e.g., AWS Glacier); > tape retrieval in the case of "offline" backups. ■ Bandwidth and latency of the internet connection in the case of "online" backups.	
Solutions	A WORM [9] solution is feasible, but it is crucial to assess the immutability mechanism [10] , as its robustness varies depending on the technologies used: ■ software protection (application code) or hardware protection (disk lock); ■ distinct technical accounts and RBAC rights for write-once operations (backup) and multiple-read operations (restoration).	An offline backup solution is still deemed as more robust than an online WORM solution. However, an acceptable compromise might be to perform regular backups using a WORM solution and conduct offline backups at a lower frequency.

Table 2 – Risks and solutions for backups in an unmanaged environment

11. *Write once read many.*
12. The concept of immutability prevents any modification of the data once it has been written to the storage medium, and ensures the integrity and availability of the data during subsequent read operations.

Version 1.1 - 27/11/2025 - ANSSI-BP-100-EN

ISBN : 978-2-11-167146-1 (numérique)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité